

ABSTRACT OF THE DISCLOSURE

5 A modular multiplier and an encryption/decryption
processor using the modular multiplier, which is mainly
applied in a chip to have the needs of small size and faster
operation. In the modular multiplier, Montgomery algorithm
is realized, the operand is divided into the fixed-length
data, and the desired result is provided by the iterative
calculation. In the algorithm, two recursive structures
include the multiplication operation first and the addition
10 operation later. By the multiplexer to data path's choice,
the desired result of modular multiplication can be
calculated by a single data path at different time points.